CLAIMS:

What is claimed is:

1. A method in a first server data processing system for responding to a denial of service attack from a client, the method comprising:

detecting an occurrence of the denial of service attack from the client in which credentials are presented to the first server data processing system by the client;

responsive to detecting the occurrence, blocking connections from the client to the first server data processing system;

responsive to detecting the occurrence, replaying an instance of the denial of service attack to a second server data processing system; and

responsive to a failure of the instance of the denial of service attack on the second server data processing system, sending a command to the second server data processing system to block connections from the client.

2. The method of claim 1, wherein the replaying step comprises:

presenting the credentials to the second server data processing system.

3. The method of claim 2, wherein the failure of the instance occurs if the second server data processing system fails to accept the credentials.

4. The method of claim 1 further comprising:

repeating the replaying step and the sending step for a set of server data processing systems.

5. The method of claim 1, wherein the detecting step comprises:

receiving the credentials from the client;

determining whether the credentials are valid; and

responsive to the credentials being invalid credentials, determining whether the denial of service attack from the client is occurring in response to receiving the invalid credentials.

6. The method of claim 5, wherein the step of determining whether the denial of service attack from the client is occurring in response to receiving the invalid credentials includes:

determining whether a number of the invalid credentials received from the client has exceeded a threshold selected to trigger a presence of the denial of service attack.

7. The method of claim 1 further comprising:

responsive to receiving the command from another server data processing system, blocking connections from the client.

8. The method of claim 1, wherein the command includes an instance of the denial of service attack and wherein the method further comprises:

responsive to receiving the command from another server data processing system, replaying the instance of the denial of service attack to the second server data processing system; and

responsive to the failure of the instance of the denial of service attack on the second server data processing system, sending the command to the second server data processing system to block connections from the client.

9. A data processing system in a first server data processing system for responding to a denial of service attack from a client, the data processing system comprising:

detecting means for detecting an occurrence of the denial of service attack from the client in which credentials are presented to the first server data processing system by the client;

blocking means, responsive to detecting the occurrence, for blocking connections from the client to the first server data processing system;

replaying means, responsive to detecting the occurrence, for replaying an instance of the denial of service attack to a second server data processing system; and

sending means, responsive to a failure of the instance of the denial of service attack on the second server data processing system, for sending a command to the second server data processing system to block connections from the client.

10. The data processing system of claim 9, wherein the replaying means comprises:

presenting means for presenting the credentials to the second server data processing system.

11. The data processing system of claim 10, wherein the failure of the instance occurs if the second server data processing system fails to accept the credentials.

12. The data processing system of claim 9 further comprising:

repeating means for repeating initiation of the replaying means and the sending means for a set of server data processing systems.

13. The data processing system of claim 9, wherein the detecting means comprises:

receiving means for receiving the credentials from the client;

first determining means for determining whether the credentials are valid; and

second determining means, responsive to the credentials being invalid credentials, for determining whether the denial of service attack from the client is occurring in response to receiving the invalid credentials.

14. The data processing system of claim 13, wherein the second determining means includes:

means for determining whether a number of the invalid credentials received from the client has exceeded a threshold selected to trigger a presence of the denial of service attack.

15. The data processing system of claim 9, wherein the blocking means is a first blocking means and further comprising:

second blocking means, responsive to receiving the command from another server data processing system, for blocking connections from the client.

16. A computer program product in a computer readable medium in a first server data processing system for responding to a denial of service attack from a client, the computer program product comprising:

first instructions for detecting an occurrence of the denial of service attack from the client in which credentials are presented to the first server data processing system by the client;

second instructions, responsive to detecting the occurrence, for blocking connections from the client to the first server data processing system;

third instructions, responsive to detecting the occurrence, for replaying an instance of the denial of service attack to a second server data processing system; and

fourth instructions, responsive to a failure of the instance of the denial of service attack on the second server data processing system, for sending a command to the second server data processing system to block connections from the client.

17. The computer program product of claim 16, wherein the third instructions comprises:

sub-instructions for presenting the credentials to the second server data processing system.

18. The computer program product of claim 17, wherein the failure of the instance occurs if the second server data processing system fails to accept the credentials.

19. The computer program product of claim 16 further comprising:

sub-instructions for repeating initiation of the third instructions and the fourth instructions for a set of server data processing systems.

20. The computer program product of claim 16, wherein the second instructions comprises:

first sub-instructions for receiving the credentials from the client;

second sub-instructions for determining whether the credentials are valid; and

third sub-instructions, responsive to the credentials being invalid credentials, for determining whether the denial of service attack from the client is occurring in response to receiving the invalid credentials.

21. The computer program product of claim 20, wherein the third sub-instructions includes:

instructions for determining whether a number of the invalid credentials received from the client has exceeded a threshold selected to trigger a presence of the denial of service attack.

22. The computer program product of claim 16 further comprising:

fifth instructions, responsive to receiving the command from another server data processing system, for blocking connections from the client.

23. A data processing system comprising:

a bus system;

a memory connected to the bus system, wherein the memory includes a set of instructions; and

a processing unit connected to the bus system, wherein the processing unit executes a set of instructions to detect an occurrence of a denial of service attack from a client in which credentials are presented to a first server data processing system by the client; block connections from the client to the first server data processing system, in response to detecting the occurrence; replay an instance of the denial of service attack to a second server data processing system, in response to detecting the occurrence; and send a command to the second server data processing system to block connections from the client, in response to a failure of the instance of the denial of service attack on the second server data processing system.